The Economics of Y2K and the Impact on the United States

0.



AND STATISTICS ADMINISTRATION

U.S. Department of Commerce

November 17, 1999

THE ECONOMICS OF Y2K AND THE IMPACT ON THE UNITED STATES



Economics and Statistics Administration U.S. Department of Commerce

November 17, 1999

The Economics of Y2K and the Impact on the United States was prepared under the direction of Robert J. Shapiro, Under Secretary of Economic Affairs, Economics and Statistics Administration and Lee Price, Chief Economist. William B. Brown and Laurence S. Campbell were the primary authors.

Questions concerning the content of this report should be directed to the Office of the Chief Economist, Room 4842, U.S. Department of Commerce, Washington, D.C. 20230. Phone: (202) 482-4885.

Foreword by Robert J. Shapiro

For the United States, the Y2K problem is something like a tangled shoelace for a world-class marathon runner. The world's most technically sophisticated and information-technology intensive economy faces real disruptions, when billions of software programs and microprocessors turn over from the final moment of 1999 to the first moment of 2000. Fortunately for the marathon runner, it is a long race, and American firms and government agencies appear to be doing what they need to do to prevail. Forecasts of the costs of Y2K disruptions to the American economy range from mild to severe, with recent studies generally concluding that Y2K glitches should cost the United States less than many analysts had once anticipated. The truth is, no one knows with certainty what the precise economic consequences will be. *It is our best judgment that Y2K problems will not be of sufficient size or scope to have more than a transient effect on U.S. economic growth.*

The greatest costs to the American economy from the Y2K problem have probably happened already. To find and fix their Y2K problems, businesses and government agencies have diverted in the neighborhood of \$100 billion from other purposes in recent years. This substantial commitment reflects millions of business judgments, in which firms recognized that failing to protect their critical systems would, in our highly-competitive and transparent market economy, expose them to significant costs. The available evidence suggests the sectors that have invested the most and are now best prepared are those that provide the critical goods and services on which the rest of the economy depends—energy, finance, telecommunications, and transportation. The least prepared seem to be the education and health care sectors, smaller businesses and agencies, or non-critical systems. In these cases, the glitches that will show up are likely to have limited effects beyond the specific businesses, and are likely to be fixed reasonably easily and quickly once they are identified.

There will be additional economic costs associated with Y2K problems in the United States. Some firms will spend less than they need to, and some will have spent too much. In both cases, profits and jobs will be affected. Moreover, there are many important unknowns which should make anyone cautious about predicting Y2K's full impact on the economy. Economic forecasting tends to be most accurate when past experience provides several previous occasions when the same key variables were present and aligned in ways that resemble the present. Unfortunately, there are no close historical analogies to Y2K, nor any data from similar transitions in the past to help predict the likely consequences.

Some early analysts tried to construct analogies between Y2K and natural disasters, but the similarities are small. Unlike most natural disasters, which generally occur with little warning, business, government and much of the American public have all known about Y2K for years. Because the problem has been widely recognized, private firms and governments have had real incentives to fix their problems — which in turn is the primary reason why Y2K does not now appear to pose a real economic threat. In addition, unlike most natural disasters which do their damage quickly, the Y2K problems are unfolding over a much longer period of time than is commonly appreciated. Because Y2K glitches can be triggered any time computer chips or software programs encounter a year 2000 reference, many firms already have experienced some errors. Most reports indicate that these problems have been addressed quickly and without significantly disrupting ongoing operations. Further, unlike most natural disasters which are

geographically concentrated, Y2K problems are worldwide in scope with literally millions of technicians ready to pounce on problems as they occur. While American firms may be disrupted by Y2K glitches in distant countries, those that depend on cross-border linkages, such as banks and traders, also have back-up systems, contingency plans, or have increased their inventories.

In one respect, the comparison of Y2K to a natural disaster is fairly apt. If a natural disaster is big enough, it will affect the timing of economic growth and national output – but not the overall total. Initial declines in output and growth associated with the disaster are offset by subsequent recovery activities. In a similar way, concerns about Y2K problems are apparently affecting the timing of some inventory purchases, investments, and employment demand for programmers. In an economy as stable, large, and resilient as America's, however, single events almost never affect total GDP for very long. In our best judgment, Y2K will not be an exception to this rule.

We have pursued this project to investigate the economic implications of Y2K on the U.S. economy at the request of the President's Council on Year 2000 Conversion and in close partnership with its Chair, Dr. John Koskinen. We are pleased that, since the initiation of our analysis for the report, the Senate Special Committee on the Year 2000 Technology Problem has also expressed interest in its publication.

EXECUTIVE SUMMARY

As a result of programming decisions made during their creation, computer software and hardware may not recognize the Year 2000 accurately, causing operational errors. This report assesses the economic implications of this Y2K problem for the U.S. economy. The Department of Commerce's Economics and Statistics Administration reviewed how firms and governments should be expected to react in the face of the knownY2K problems and compared these results with available progress reports on Y2K readiness and other published Y2K economic assessments.

Overall Assessment & Key Judgements: Y2K is having an impact on U.S. business activity well in advance of the actual 1999 to 2000 changeover. Expenditures by firms and public agencies to hunt down and correct error-prone technologies have been running on the order of \$30 billion a year since 1997 and will total in the neighborhood of \$100 billion. Since the economy is essentially fully employed, the Y2K expenditures are coming at the expense of productivity-enhancing investments and consumption. Once Y2K is resolved, more resources will be available for both.

It appears that Y2K problems will not be of sufficient size or scope to have more than a transient effect on overall U.S. economic growth. With no shortage of information about the problem, firms are correcting what is clearly a messy but not intractable situation. Y2K readiness and assessment reports by government agencies, the private sector, and private consultants are, for the most part, optimistic. While international organizations have reported a lower level of Y2K preparedness in many foreign countries, the countries that are highly dependent on information technology, and thus exposed to substantial risks, are reported to be well along with their fixes. There appears to be little chance that Y2K disruptions abroad will be transmitted to the United States to a degree that could substantially damage the economy. There are still important unknowns, and no one knows with certainty the precise economic consequences. However, the U.S. economy has faced many such pressures and has proven to be highly resilient in recent years.

How Firms Can Be Expected to React to Y2K: At the firm level, the Y2K problem is not that different from other risks businesses face every day. Firms can be expected to balance, from their own points of view, the perceived costs and benefits of identifying, fixing, and testing for Y2K problems and developing contingency plans.

- In competitive markets, where it is difficult to pass on new costs to customers, firms can be expected to spend enough to avoid significant losses while accepting a risk of some failures. The level of precautionary Y2K spending among firms may vary, depending on the degree of a firm's risk aversion and its financial means.
- In more concentrated markets, where there is a greater ability to pass on costs, firms can be expected to make efforts to figure out what their competitors are doing, and defensively to copy that behavior. The variation in spending between firms will probably be less in these more concentrated markets.
- For well regulated markets and government agencies, where there is a greater ability to pass on costs and where a sustained Y2K failure could be severely disruptive for others, there will be a strong incentive to find and fix all Y2K problems. But in countries that are poorly governed, or where monopoly firms or public services are poorly managed, these are the areas of greatest risk.

Clearly, some firms will make rational choices that include risks of failures. Some of these decisions will end up being wrong, and some profits and jobs will be affected as a result. It is unlikely these errors will be large enough to cascade into an economy-wide disruption, but this is not knowable with certainty.

Economic Basis for the Governmental and Public Role in Y2K: Even with the best of intent and the most rational decisions possible, the effects of these firm-level Y2K remediation decisions on the general economy could be influenced by special factors. Clearly, any sustained failure in critical infrastructure system, such as telephone or electricity, would be very disruptive, could have cascading effects, and is outside the control of most firms. Misinformation about the Y2K problem or the state of its resolution—whether or not the misinformation is deliberate—could lead to incorrect actions or levels of investment in Y2K fixes. Also, private decisions on Y2K spending can have good or bad effects on the broader society. Left to their own devices, firms might choose Y2K strategies that, while rational from their view, could still have negative implications for other people.

The potential for these factors to influence private Y2K decisions provides a strong public policy justification for the executive and legislative branches of government, industry regulators, industry associations and consultants, and the media to pay close attention to Y2K vulnerabilities. Public scrutiny has increased the level of private investment in fixing Y2K, thus reducing the potential external effects on society as a whole. In principle, governmental activities intended to mitigate the impact of the problem could also encourage behavior that makes the problem more likely. Government Y2K policies and programs have tried to avoid the danger of such "moral hazard" by insisting that responsibility to fix Y2K problems lies with the individuals, firms and agencies involved.

Domestic Y2K Readiness: The Y2K-problem is, at its core, a technological error that can be tested and corrected. By most accounts, the domestic U.S. economy is generally well-prepared.

The President's Council on the Year 2000 Conversion believes that "important national systems will make a successful transition to the Year 2000," and that it has a "high degree of confidence" in financial institutions, electric power, telecommunications, and the federal government. The Senate Special Committee on the Year 2000 Technology Problem concludes that sectors "critical to the safety and well-being of Americans, as well as to the economy, have made significant progress in the last eight months...". Both reports indicate continuing concern for certain domestic sectors, including health care, local government, small business, and education, without however, finding general economy-wide risks. Private sector Y2K consultants and polls on corporate Y2K readiness, with a few exceptions, have the same general views.

An additional consideration supports these optimistic assessments: Surveys suggest that the majority of firms have already experienced some Y2K failures, and reports indicate that these have produced temporary, fixable disruptions. There will be a spike in failures at the turn of the year, but it may not be as large or as significant as commonly expected.

International Y2K Readiness and Implications for the U.S. Economy: Some concern remains about the level of international preparations and how foreign Y2K problems might effect the U.S. economy. However, for the most part, economically-sound behavior appears to be occurring overseas as well. U.S. firms that depend on suppliers overseas have a strong incentive to make sure that they are Y2K ready and that there are contingency plans in place–e.g., inventories,

alternative suppliers–in case there are Y2K related disruptions. No information indicates that U.S. firms are doing less overseas than they are doing domestically.

Overseas problems are most likely to occur in countries with highly centralized, poorly supervised organizations and where there is current, severe economic distress. However, these nations do not play a major economic role in the U.S. economy. The major U.S. trading partners of Canada, Mexico, Europe, and Japan–where information technology plays a large role in the economy–report a strong degree of preparation and Y2K readiness.

For a foreign nation's Y2K failures to present a sustained threat to our economy, the foreign nation and its firms would have to be IT-intensive, very poorly Y2K prepared, important economically to the U.S., *and* have significant Y2K-related links that could generate sustained economic disruption. Available country-level assessments do not indicate any nations where all four of these risk factors to the U.S. are present.

The structure of economic incentives to U.S. firms, the reports of U.S. firm-level preparations involving the overseas supply chain, and country-level assessments of the major U.S. trading partners are consistent with the expectation of transient effects in trade-dependent sectors of the U.S. economy. Additional inventories, contingency preparations, and the time lags between foreign production and domestic use suggest that disruptions abroad should not immediately affect U.S. producers and ultimately, may not affect them very much. Trade takes place between tens of thousands of individuals and firms, and that is where Y2K readiness, contingency planning, and response to any glitches when they occur will rest. The incentive to get fixes or work-arounds in place quickly will be very high.

Estimates of U.S. Y2K Spending: Cumulative U.S. spending to address the Y2K problem is difficult to estimate. However, based upon several methodologically conservative estimates, cumulative Y2K readiness spending appears to be in the neighborhood of \$100 billion, or about \$365 per U.S. resident. Y2K spending, which started as early as 1995, appears to have peaked in 1998 and 1999 at about \$30 billion per year.

Effects on Productivity: Spending to fix the Y2K technological errors increases costs and creates a diversion of spending from other productive investments. Some of the Y2K spending may involve 'shifting forward' new, productive, software and hardware investments which would have occurred eventually, offsetting to some extent the drag on productivity. Because Y2K spending has occurred over a number of years and is small relative to the economy, it is difficult to estimate the extent of productivity effects with assurance. For the future, the lifting of the Y2K repair burden should free resources that can be used in ways that will raise productivity.

Inventory and GDP Effects: Y2K contingency planning by firms and Y2K-related consumer behavior may have implications for inventory shifts and the composition of GDP at the turn of the year. Because of these issues, consensus economic forecasts anticipate some inventory build-up now, offset by a reduction in the early part of next year. Also, Y2K contingency planning may involve, at least for some firms, a 'lock-down' that could reduce installations, if not orders, of software and hardware from what they otherwise would have been in the fourth quarter of 1999. As with the productivity effects, it will be very difficult to estimate after the fact these inventory and capital spending effects with either precision or assurance.

Consumer Behavior Concerns: A sudden rise in risk aversion associated with Y2K concerns translated into unusual demand for cash or household goods—could prove disruptive to finance and commerce even with advance preparation. Current polls, however, suggest that the public is becoming *less* worried about Y2K as the date approaches. And financial institutions appear to be among the best prepared for Y2K. Most importantly, even if risk aversion rises, two-way markets ensure that the choice of holding more cash or hoarding goods will come at higher prices that reward those who accept modest risks.

Need to Avoid Complacency: While the general assessments of Y2K readiness and the implications for the U.S. economy as a whole are optimistic, Y2K glitches will surely happen and disrupt the firms and individuals involved. All firms and individuals should be sure that they have taken steps to identify, fix and test for Y2K problems, and put in place appropriate contingency plans.

TABLE OF CONTENTS

| Foreword by Robert J. Shapiro |
|---|
| Executive Summary |
| INTRODUCTION: THE Y2K GLITCH |
| FIRST ORDER FAILURES AND THE PROBLEM OF INTERFERENCE 7 Timing of failures 7 Types of failure 7 Duration of failure 7 |
| WHY MOST FIRMS WILL COPE WITH Y2K: THE CENTURY DATE CHANGE AS A MICROECONOMIC ISSUE Firms in very competitive markets Firms in highly concentrated markets Highly regulated firms Consumers and investors |
| TAKING CARE OF BUSINESS: THE MACROECONOMICS OF Y2K 7 Critical Infrastructure 8 False Expectations and Misinformation 9 Externalities 9 Moral Hazard 10 |
| ASSESSMENTS OF Y2K READINESS IN THE UNITED STATES |
| U.S. VULNERABILITY TO Y2K PROBLEMS ABROAD |
| CONCLUSION: DIRECT EFFECTS OF Y2K ON THE AMERICAN ECONOMY 2 Disrupted Output 2 Y2K Inventory Shifts. 2 Consumer Responses. 2 The Costs of Fixing Y2K. 2 Summing up, The Impact on GDP 24 |

INTRODUCTION: THE Y2K GLITCH

When economists or business analysts first look at the Y2K problem, it appears to many as a trivial anachronism left over from the times when computer memory was expensive. With memory now cheap, and with new systems being introduced all the time, Y2K sounds like a messy but rather everyday kind of problem. Indeed, for most individuals and for most small operations this is largely the case. But this view can be misleading if it loses sight of the history and complexity of the development of this still new information technology industry. The practice of using two-digits to identify a year-date in software and in microprocessor chips began in the 1950s and 1960s, when much of this work was experimental and informal and when the year 2000 was considered too distant to justify the added expense of recording and processing all four digits for the year-date. Not until recent years could most code-writers imagine how successful their projects had been and how pervasive and essential the information technology industry that they created would become, worldwide. Nor could they visualize the havoc that their shorthand manner in setting dates could play in an economy, if not corrected.

The Y2K Glitch

The year 2000 programing error occurs when computers or microprocessors fail to make the correct transition from 1999 to 2000. It is the result of use from the 1950s through the early 1990s of a two digit representation for the year in calendar or timing devices (for example, 99 for 1999), rather than four digits. Even in applications that may not seem to be year sensitive, timers are often used that include a two-digit year followed by days, hours, minutes and seconds to regulate periodicity, and these can malfunction when the clock transitions through the millennium turnover—in effect, turning 99.9999 to 00.0000. Such malfunctions may not occur at the actual New Year, since the original set-time of clocks varies, time zones differ, and many applications require calendar data well ahead of the new year.

To be certain that a system is Y2K compliant, a programmer must often search for the date error in millions of lines of software code, and in data sets where only 2 digits are available for birth years and the like. In an industrial application, technicians must determine whether embedded chips-often the proverbial black boxes of modern machinery are susceptible to the date error, and apply one of several possible fixes to remove or work around the problem. Remediated software and hardware must be extensively checked to insure that new problems are not introduced by the correction. The majority of the total costs of fixing Y2K are entailed in this search for errors and testing the remedy applied. The actual fixes and work-arounds are relatively inexpensive. As the year 2000 approached, the problem clearly became non-trivial: U.S. Fortune 500 firms alone are spending upwards of \$35 billion to ensure the smooth processing of dates in 2000 and beyond. Individual firms such as GM and Proctor and Gamble report spending \$600 million over several years. Large foreign firms have spent comparable amounts. US banks collectively are spending more than \$9 billion to assess, fix, and test their systems. In the public sector, the U.S. Air Force is spending \$1.2 billion, and the Federal government will spend more than \$8 billion on Y2K¹.

The nature and dimensions of the Y2K economic challenge arise from several specific technical characteristics.

Legacy software. Information technology hardware and software have evolved so continuously over the past 25 years that new applications have been incorporated by modifying slightly older versions of

programming and records. The result is that very few systems are completely devoid of code or records from the 1970s and 1980s, when the century turnover seemed too distant to worry about. Further, in the rigorous and non-reflective manner in which microprocessors and computers operate, even one line of code that has not been touched in decades can disrupt or shut down a system, or produce error-laden results.

Embedded chips. Billions of microprocessors produced over the past 30 years include clock chips, many costing less than \$1.00 to produce, set at "absolute time" beginning with a two-digit year-

¹ OMB 10th Quarterly Report: Progress on Year 2000 Conversion, September 13, 1999.

date followed by months, days, hours, seconds and sometimes milliseconds. Most of these chips have been used in watches or other applications that do not carry risks of causing a cascade of problems. Many, however–no one really knows the number–have been embedded in a wide range of equipment as convenient timing devices for industrial applications. By subtracting one absolute time from another, for instance, a typical device derives elapsed time for the flow rates in a pump, the timing circuit in a traffic light, or the interval between moving trains. If the device is operating when the year date for the end time shifts from '99 to '00, a malfunction may occur as the device reads an extremely long interval of time or time running backwards. However, if the device is not in operation when the clock turns from 99 to 00, both the start time and the end time may register the same century and the device could continuing operating correctly. These vagaries in results mean that diagnostic costs for this problem are often steep and the consequences unknown. For these reasons, many businesses are dealing with embedded chips by replacing the equipment or by adopting an approach of simply fixing devices after they fail.

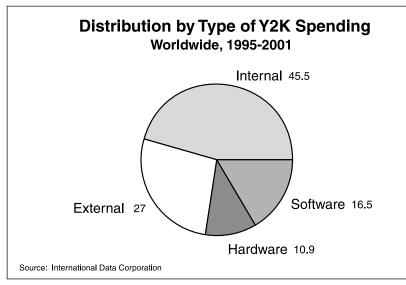
The complexity of software. Software can extend to millions of lines of code and thus are among the most complicated products ever devised. As a result, they are notoriously susceptible to errors when any element is changed. Moreover, software changes constantly with use, so that rarely are two units identical. Ironically, much of this software is also not easily searched electronically for the dating element, and sometimes thousands of worker-hours are required to track down potential two-digit date errors.² Once corrected, much testing is needed to insure that the remedy works and does not itself introduce new problems. Some information technology experts have found that five to ten percent of software that has been fixed and extensively checked is still defective in some way. Experience gained from several years of testing, however, and the development of new tools specifically designed for Y2K testing of various programing languages have greatly improved the ability of analysts to at least audit corrections if not fix them entirely.

Open systems. With some exceptions, the computer and software industries have developed along the lines of "open systems", in which many vendors provide add-ons to the basic architecture. The open character of these systems makes it more difficult to diagnose hardware and software for Y2K problems. At the same time the great variety of applications that are subsequently developed for open systems also reduce the potential that large numbers of applications will be affected the same way, crashing simultaneously in a cascading fashion.

Linkages. A Y2K error in one application or device is not a "virus" that can actively invade other parts of an IT system. However, the pervasive use of information technology entails extensive exchanges of information through complex networks, and a breakdown in one application can impact others very quickly. For example, a Y2K failure at a credit check facility could prevent the use of an otherwise unrelated credit card. However, as with open systems, networks and linkages also often introduce redundancies in business operations that may reduce the cost of a Y2K-related failure. For instance, the widespread use of ATMs or money cards greatly increases redundancy in retail transactions, protecting retailers against the loss of billing records in a Y2K breakdown. And information technologies have given consumers much more redundancy in tools they can use to make transactions, rather than depending on cash or checks.

Costs of diagnosis, repair, and testing. Y2K problems, once identified, can usually be fixed quite readily using several possible patches or "work-arounds." The largest costs involve identifying

² For example, Union Pacific analyzed 7,000 COBAL programs totaling 12 million line of executable code. It estimated it would take 200,000 man- hours, or 100 staff each working for a year, to convert these programs. JP Morgan.com, July 21, 1999.



and diagnosing the problem, especially in the case of embedded chips, and in testing the applications once they have been fixed, especially with software. Some experts estimate that up to one-half of the total costs of Y2K remediation are in testing, since a fix for one problem may introduce new glitches. For this reason, the most cost-effective strategy for some firms is to "fix on failure," and one survey has found that about 10 percent of business are using this approach for equipment with embedded chips.³ Of course, for some operations, failures would be non- reversible and potentially catastrophic, and thus such a strategy not an option. It is even more difficult and costly to test for vulnerabilities to errors originating in systems

outside a firm, forcing many businesses to resort to contingency planning rather than pursue upstream and downstream vulnerabilities.

FIRST ORDER FAILURES AND THE PROBLEM OF INTERFERENCE

Given these characteristics of the Y2K problem, the nature of specific Y2K failures is fairly simple to describe. It is more difficult to determine whether these discrete failures are likely to influence each other and create more substantial economic damage by interfering with systems that have not failed. Critical to this issue is the degree to which failures will occur all at once, the types of failures that do occur, and how long they persist. The evidence suggests that Y2K failures: a) are likely to be spread over more time than many have expected; b) are likely to be of minor consequence if they remain discrete; c) have a potential for creating substantial confusion in operations when they occur simultaneously; and d) after failure can be fixed fairly quickly.

Timing of failures. By definition, Y2K is a time-defined problem that will peak in the hours before and after the century mark is reached. Cascading problems associated with the date change, if they are to occur, are thus expected in the first days of the New Year. This is particularly true of most of the embedded chips that do turn out to have the transition problem–although such chips can be set at any one of many of the world's time zones. And some chip failures could occur years later if their start dates were set arbitrarily at the time they were set up–since the year-date itself in most situations other than the century date change may be irrelevant to the workings of the device.

Software, however, is a somewhat different story. The proportion of all software failures that are likely to occur just before and after midnight December 31, 1999 is probably smaller than generally believed. Y2K risks rise steeply in the fourth quarter of 1999, as year 2000 fiscal years begin and as software starts looking for next quarter or next month dates. After peaking at the

³ In testimony given to Senate Special Committee on Y2K Problem, July 22, 1999

time of the century date change, additional problems will continue to show up throughout the year. February 29th, 1999 is a particular problem since calendars that simply substituted "20" for the "19" digits might not recognize that there will be a February 29, 2000; there was no February 29, 1900. ⁴

Errors that occur before the century-date change often are associated with forecasting and scheduling activities that may not be critical to an organization's basic operation. Similarly, errors that occur well after the century-date change may be numerous, but are also less likely to be of a critical nature. By 2001, the problem should be essentially over.

Types of failure The scale of potential damage to a specific operation from Y2K errors is very difficult to predict, adding much to the uncertainty of the whole event. Individually, the errors tend to be of minor consequence but if they occur simultaneously they can quickly add up to great confusion within a system that depends on information technology. To date, Y2K failures have been generally minor and quickly corrected. And after extensive analysis, some firms have decided that their Y2K problems are less serious than they had anticipated. Ford Motor Company, for example, concluded that despite widespread use of embedded chips since the 1980s, there were no latent problems with the operation of its automobiles. A more integrated operation, for instance the entire process of building and selling automobiles, carries much more risk of simultaneous errors cascading into a very serious problem-enough that automakers have felt the need to spend hundreds of millions of dollars to make sure they are Y2K ready. In worst case situations, the permanent loss of data or the shut-down of critical systems remains possible. Given these uncertainties, firms generally have divided their potential problems into "mission critical" and "mission non-critical" classes. Much of the non-critical work has been left for the last minute or postponed into the new year, when at least the cost of identifying and diagnosing the problem will be much less. For this reason we will continue to see Y2K errors and expenditures well into the new year.

Duration of failure. There is little evidence that Y2K failures are likely to cause prolonged shutdowns. Barring secondary or cascading problems, most Y2K failures can be corrected quickly. With many "embedded chips," for example, failures should occur once and only over the exact period that the date turns over. In many such cases, the remedy may involve simply turning the system or equipment off and on again. Even as problems are diagnosed, however, there will no doubt be many frustrations as orders for hardware or software "patches" surge and bottlenecks develop. Already many devices are on lengthy wait lists, causing firms to develop temporary workarounds.

Other aspects of the duration of errors should limit the damage. Firms are engaged in an intensive process of preparing contingency plans and most providers of information services expect to be on alert over the New Year holiday and well into the first two weeks of January.⁵ Further, January 1, 2000 falls on a Saturday, providing an extra day to address simple mechanical glitches before most Americans return to work on Monday, January 3rd. In other countries even more latitude is gained by having January 3rd the New Year's holiday, versus Friday, December 31st in the United States. Of course the holiday period raises peak demand for some types of services, especially demand for long-distance telephone at the point of the New Year, leading to a likelihood of overtaxed systems even without the Y2K problem.

⁴ Since the earth's rotation around the sun takes slightly less than 365.25 days, years ending in 00 are not leap years except for years divisible by 400.

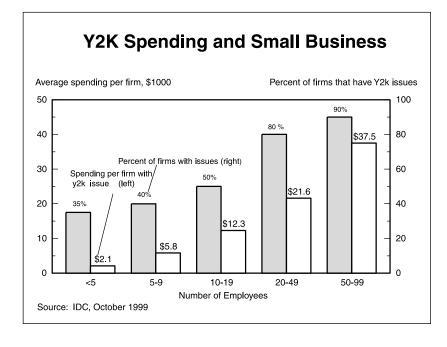
⁵ Japan, for example, plans to have 100,000 information technology personnel on call New Year's Eve.

WHY MOST FIRMS WILL COPE WITH Y2K: THE CENTURY DATE CHANGE AS A MICROECONOMIC ISSUE

From the perspective of an individual firm, in the United States and elsewhere, the Y2K problem is not very different from other business problems faced every day. Many business analysts would argue the only exceptional aspect of the Y2K problem is its world-wide scope and the fact it is associated with a change in millennia which has captured the public imagination. Nevertheless, Y2K does present some real problems for literally millions of firms, worldwide. Individuals and firms lack perfect knowledge of their systems, tests rarely if ever cover all contingencies, and many will take risks. With any problem as pervasive as this one, some firms will not make the correct decisions, and jobs will be affected. It is even possible, although not likely, that some catastrophes may occur.⁶ But an economy-wide disruption is unlikely, given the redundancies and resilient nature built into competitive market economies.

Most firms and individuals have enough at stake in correcting their own Y2K problems that their individual responses, taken together, will avert an economy-wide impact, at least in the United States. This is the nature of our economic system, of strong competition coupled with regulation. Moreover, the theory that firms have ample incentive to solve their own Y2K problems is supported by the evidence of what they have actually been doing.

Looking at the Y2K issue through this microeconomic lens will also help identify the risks to the economy that remain and where to look for danger signs or anomalies. In doing so, it is helpful to distinguish among four types of actors in the economy, including producers and consumers, to examine how each, acting in their own best interests, can be expected to respond to the Y2K challenge.



1) Firms in competitive markets. Competition forces such firms, including most small businesses, to explicitly measure the economic costs of fixing their systems against the risk and cost of failing to do so. These firms can lower the risk of failure of their own systems, perhaps to zero, by spending more money. They can also reduce the risk of outside forces affecting them, but not completely eliminate it, through contingency planning and stockpiling. But spending too much also presents a risk. Unless all their competitors in the industry use the same technology and make the same decisions, the firm will not be able to pass on to consumers the cost of fixing their Y2K problems. Competition thus forces these firms to divert their Y2K funds from other investments or from profits. The key decision for a firm in a competitive markets is how much protection it should purchase.

⁶ For instance, a Texas A&M survey of small and medium chemical firms in October 1999 found that 4 percent of the respondents felt that there was some potential for catastrophe at their plants, given a worst case situation. Forty seven percent felt their plants would see nothing in the way of bad results, 30 percent felt some economic disruption was possible. The others had no opinion.

Since a large share of Y2K remediation costs are precautionary, much like insurance, competitors with different degrees of risk aversion will make different choices and so may end up being affected very differently. A firm that chooses not to spend funds "insuring" itself against potential Y2K problems and which, by good fortune, does not experience Y2K problems, may gain a competitive advantage over a firm that has spent part of its investment on ensuring itself against internal Y2K risk. But if a firm chooses not to address potential Y2K problems and loses the gamble, its Y2K disruptions could cost it the confidence of its customers, perhaps doing lasting damage. Most firms can be expected to spend enough to avoid catastrophic losses while accepting a risk of some failures that they expect to be able to handle. A firm with strong profits or a highly-valued reputation may tend towards larger Y2K spending; while a business in trouble may tend to use its funds to stave off its creditors and assume a higher Y2K risk.

2) Firms in highly concentrated markets. Firms in concentrated markets have more control over their prices and therefore may address Y2K problems differently than businesses in more competitive markets. The central decision for this type of firm is what other large players in the industry are doing. If each of three major producers of a particular good spends roughly the same amount per good to address their Y2K problems, each will be able to pass along to consumers most of these costs. But if only one of them spends the funds, it may not be able to pass along any of the cost. On the other hand, if only one firm in such a market chooses not to invest in remedying its Y2K problems and it runs into serious problems, its reputation among potential customers will probably suffer. Finally, if no firm in such a market invests in remediation and all face Y2K production difficulties, shortages of their products would develop, causing their prices to rise, offsetting to a degree the costs of the failure. Firms in concentrated industries, therefore, tend to make considerable efforts to determine what their competitors are doing and frequently try to match their behavior. In many cases, the pace in such industries is set by a dominant leader, and its decisions largely determine how Y2K issues are investigated and resolved in the industry. For these reasons, public scrutiny of concentrated markets is needed to encourage private decisions made within these industries to correctly weigh the external costs and benefits of their decisions.

3) *Highly regulated firms with monopoly or near-monopoly power and government agencies.* Firms or agencies that provide a monopoly service also respond distinctively to the Y2K challenge. Since the actions of such organizations often can affect the economy as a whole — i.e., they produce externalities — the decisions of these firms are particularly important. Most critical infrastructure firms, such as utilities and local telephone companies, fall in this category, and most governmental regulatory attention, both in the United States and abroad, to Y2K has focused on them.

A monopoly firm can more easily pass on both the costs of remedying its Y2K problems and the cost of failing to do so, so its decisions may depend less on the potential impact on profits or market share and more on how the firm's owners or regulators view their personal risks.

In most instances, regulatory oversight reinforces the incentive to prepare for Y2K — from the actions of state utility regulators in the United States to tough administrative sanctions put in place in China for managers who allow their organizations to experience Y2K failures. But in some cases, especially in the former Soviet Union, responsibility for failures can be diluted, leading to higher risks of large Y2K failures.

What is Critical?

"Critical" means different things to different people.

For a firm, a "mission critical" operation is one where a Y2K failure would shut down production or delivery, create a health hazard, cause considerable loss of revenue, introduce substantial litigation risks, or risk significant loss of customers.

• To a telephone company, for example, a mission critical failure could be one that interfered with its ability to time calls and thus properly charge for them.

• By contrast, a telephone customer would see a "mission critical" failure as one that interfered with his or her ability to make calls, a much less likely type of Y2K failure..

"Critical Infrastructure" suggests facilities whose damage due to Y2K failures would cause a wide circle of disruptions. Damages may still essentially be local, however. In an economy as large as the United States, hundreds and perhaps thousands of failures in "critical infrastructure" electricity or water systems could occur before the impact would be great enough before there would be a significant impact

Other aspects of monopoly firms may make them particularly vulnerable to Y2K problems. These firms tend to be large, use complicated proprietary software, often depend on equipment that use embedded chips, and are intensively linked to the outside world. If the firm's monopoly is the result of economies of scale or highly channeled output–a telephone line or a pipeline, for example–one failure can cascade into a systemwide problem with damaging results. Also, many such firms and agencies adopted computerization early, before the Y2K bug was recognized, and much of their software is a legacy from that era.

In other respects, monopoly organizations usually have great incentives to fix potential Y2K problems. Where maintaining their monopoly

status requires public trust, Y2K failures that erode such trust could undermine the firm's position and its executives' careers. Since regulators may allow such firms to pass on the costs of remedying these problems, and may not allow them to raise prices if unaddressed Y2K failures interrupt production, they have large incentives to fix everything.

4) Consumers and investors. Although the Y2K problem is commonly considered an issue for producers, the uncertainties that encourage firms to spend scarce resources protecting themselves also can cause consumers and investors to react more conservatively than usual creating imbalances in supply and demand if this change in behavior is not anticipated. Some consumers facing Y2K risks will react by stockpiling key consumer items and cash and perhaps reducing the risk level of their investments. And investors may seek to avoid situations where they need to borrow funds at year-end, in effect increasing their liquidity.

In a market economy, this risk avoidance will come at some economic cost. For example, riskaverse individuals will pay more for items that are being hoarded in late-1999, and other consumers will see an opportunity to purchase the same items at big discounts in January. Similarly, if asset prices weaken as a result of investor concerns about the economic fallout of Y2K, some will try to take advantage of what they see as a "buying opportunity".

Clearly though, if consumers or investors were to abruptly change their behavior due to Y2K anxieties, it could surprise the markets and cause some potentially important losses. In the United States this danger is lessened by the fact that its less regulated markets typically allow for two-way buying and selling even in extraordinary situations. Economies with less flexible markets are at more risk of dramatic price changes immediately prior to the date-change.

TAKING CARE OF BUSINESS: THE MACROECONOMICS OF Y2K

In the United States there has been no shortage of funds to fix critical infrastructure and critical pieces of legislation were passed by Congress, and signed by the President in 1998 and 1999 that

have encouraged firms to share information with both suppliers and consumers on the state of their Y2K readiness and on fixes that they have developed. The legislation also puts some limits on potential litigation against firms that are making good faith efforts to correct Y2K errors⁷.

Even as firms and individuals respond in rational and sensible ways to the Y2K threat, there remains some potential for wider economic disruptions. There are four categories of problems that could develop for a macroeconomy if government policy does not actively intervene to remove Y2K issues. These include a) failures in critical infrastructure; b) widespread misinformation that distorts public expectations; c) large Y2K externalities, in which thousands of private decisions produce perverse social results; d) and poor public policies that relieve private actors of responsibility for Y2K errors.

Critical Infrastructure

The few analysts who have predicted Y2K-related recessions in the United States or elsewhere have focused on the potential threat of critical infrastructure failures. In fact, close analysis of these concerns does not support their predictions, at least for the United States or any other developed country.

Money and payments systems. Widespread failures in a country's financial system would have immediate effects across its economy. Older financial records are potentially at risk for Y2K date errors, and problems in one institution can affect the operations of other institutions. A sudden nationwide absence of credit approvals, for example, or failures that prevented government agencies from providing transfer payments, could choke off consumer demand.

These dangers were recognized many years ago, however, and much work has been undertaken, in the United States and elsewhere to be sure financial systems are safe. The IMF, the Bank of International Settlements in Switzerland and the Federal Reserve Board of Governors all are highly confident that American financial institutions and their major foreign counterparts and partners are very well prepared. Europeans have already had some practice in this type of problem with the shift to the Euro in January 1999, which required all European banking and credit systems to review and revise their information technology (IT) operations.

Telecommunications. A prolonged interruption in telecommunications could seriously disrupt transactions in any modern, information-oriented economy. However, communications technologies are not considered to be at high risk to Y2K problems except for some embedded chips in switching equipment. A relatively small share of communications technologies are date-driven, and the newness of most communications equipment and software mitigate the threat. Most Internet services, for example, were developed after the Y2K problem gained broad recognition.

Most of the evidence, suggests that the telecommunications networks in the United States and other advanced economies are well-prepared. However, Y2K-related billing and other administrative problems could temporarily reduce the efficiency of some communications systems and cause financial problems for firms that do not prepare adequately.

⁷ The "Year 2000 Information and Readiness Disclosure Act" (Public Law S.2392) signed by the President on October 19, 1998 and "The Y2K Act (Public Law 106-37), signed by the President on July 1, 1999. See Senate Special Y2K Committee Report, "Investigating the Year 2000 Problem: The 100 Day Report", pp 155-159.

Energy. Another critical infrastructure that affects the performance of the overall economy is the electric power and other energy-delivery systems. Of all energy-supply systems, crude oil and coal appear to be the least vulnerable, due to the large volumes of these fuels kept in inventory. One legitimate concern is the widespread use of embedded chips in electric-power generation equipment and pipeline-delivery systems. Testing of some electric power plants have shown that Y2K errors, if not fixed, do have some potential for forcing a plant to be shut down. Many such systems, however, predate the information technology revolution and include many manual and electric-mechanical redundancies. The electric-power grids of virtually all developed countries provide great redundancy.

There is little evidence that Y2K problems pose a significant threat to the energy systems of the United States. In early January 2000, electric power systems should be operating at only about half their capacity, compared to their summer peaks, and will be on guard for unexpected problems. Many analysts, however, are less sanguine about potential energy system problems in a few other countries, most notably Russia.

False Expectations and Misinformation

False expectations about the Y2K problem, if widespread, could affect a national economy. If the public holds an exaggerated view of potential effects, for instance a widespread belief that key products or services were unsafe, large numbers of individuals and businesses could become overly risk-averse, reducing spending and investment to the point that affects a widening circle of business partners. Similarly, if the public holds an unrealistically optimistic view of the likely effects of Y2K, a country could become overly complacent and fail to make the needed fixes.

Neither exaggeration nor complacency appear to be a problem for the United States. The highly decentralized and relatively efficient economy provides large amounts of information through the price system. The government, media and private experts also have provided great amounts of information, mainly of a technical nature. Further, the justice system provides sanctions for disseminating disinformation that harms others.⁸ Industry leaders also have given high praise to last year's "Information Readiness and Disclosure Act" which has encouraged firm to firm sharing of Y2K related information with less fear of liability.

Earlier this year, misinformation, or lack of information about Y2K was seen as a particular problem for some countries, especially those with non-market or authoritarian arrangements, and in countries where less IT intensity gave a false sense of security. International organizations, multinational firms, and efforts by agencies of the U.S. government including the Commerce Department's International Trade Administration, USAID and the State Department have helped to narrow the information gap. In addition, mass media around the world have focused on the story and disseminated large amounts of generally reliable information.

Externalities

The Y2K problem is a classic example of a situation in which actions taken by a firm or individual can carry positive or negative implications for others. To the extent that any economic decision-

⁸ If anything, the US legal system may cause firms to understate the degree to which they think they are compliant, causing unnecessary preparations by those that depend on them. In a survey by CIO communications, for example, as presented to the US Senate Special Committee on July 22, 1999, 22 percent of firms polled said that they felt they were in better shape than their lawyers allowed them to say.

maker determines whether or not to prepare for Y2K disruptions based only on the costs and benefits to himself or herself, as is typically true in a competitive economy, the decision may be less than optimal for the society as a whole. If these externalities are widespread, the macro economy itself could be affected. (See box: What If?)

For example, according to press reports, Air Vietnam, a small airline that uses vintage aircraft that have not been certified to be free of Y2K errors, has decided to not fly on December 31st and January 1st. Presumably, the airline determined that the costs of checking, fixing and testing its systems would not cover likely earnings for those two days. By January 2nd, the firm should be able to identify problems in its own systems and air traffic control, and then can proceed to fix them. However, this approach entails negative externalities for other firms that depend on Air Vietnam customers, such as hotels, taxis, tourist businesses and so on.

Air Vietnam's two day hiatus will have little impact on Vietnam's economy since it is a small firm.⁹ If major airlines or aircraft producers took the same approach, however, the economic impact would be much greater. Fortunately, this is not happening. Boeing and Airbus, for example, have spent hundreds of millions of dollars verifying the safety of their products, and the airline industry reports that it has

What If?

To understand the economics of the Y2K problem, we should consider an alternative scenario in which individual firms had privately recognized the existence of their own Y2K problem but no public attention has occured. Each firm would have faced a decision much like every other business decision: do the benefits outweigh the costs to the firm? If the cost of eliminating the Y2K problem appeared to exceed the probability of damage occurring times the likely damage that would occur, a firm would not invest in Y2K remediation in advance. Left to its own devices, the typical firm would give short shrift to possible damage to the larger economy.

Economists use the term "externality" to describe a situation in which a private decision has economic effects (good or bad) on the broader society. The Y2K problem potentially has two major forms of externalities. First, interruption of some types of business (e.g., finance, transportation, utilities) would have an immediate effect on the general economy. Second, a large number of simultaneous Y2K failures, regardless of industry, could overwhelm the capacity for fixes and cumulate into a macroeconomic problem.

Now consider the actual situation in most countries-particularly the U.S.-today. A combination of government officials and regulators, industry associations, consultant businesses, and media coverage have created an environment of public awareness and scrutiny of potential Y2K problems. *By changing the calculus of costs of Y2K glitches, public attention has had economic consequences.* Knowing that any Y2K failures will be widely publicized, larger businesses and those with externalities (e.g., small utilities or banks) have invested more heavily in Y2K remediation than they would have in the absence of external scrutiny.

By the same token, we must recognize that external scrutiny has created incentives for businesses to assert greater confidence in their Y2K readiness than the facts may merit. Thus, we should not assume that their will be no Y2K glitches among the companies and industries now giving assurances to the contrary.

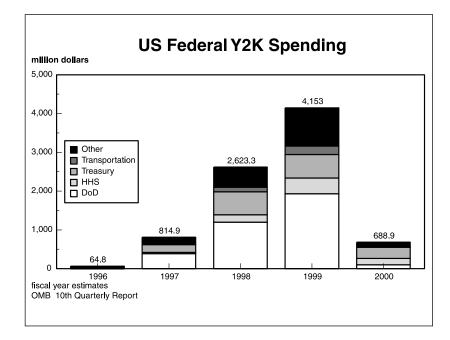
spent \$2.3 billion dollars to prepare for Y2K. Most airlines will fly over the New Year's holiday. Even with airline officials and governments guaranteeing the safety of flying, residual Y2K fears are apparently reducing demand for flights over the New Year's weekend. Other tourist-related bookings also are less than expected, illustrating the negative externalities that are posed by the Y2K issue. The existance of externalities provides an important reason for governments and large business associations to supplement the activities by the private sector to fix potential Y2K problems.

Moral Hazard

Governments can also introduce economic distortions associated with a problem that economists call "moral hazard." Moral hazard occurs when an action designed to reduce the damage from a potential problem has the perverse effect of encouraging behavior that makes the problem more likely. Insurance often involves moral hazard: a driver who knows he is covered in case of an accident may tend to drive less carefully. Bankruptcy laws, bank bailouts, and deposit insurance are common examples of government policies that increase moral hazard, but which societies accept for their larger perceived benefits.

⁹ Vietnam News" PC Week, July 21, 1999

If a government assumes too much of the Y2K burden, firms and individuals may tend to do less for themselves, creating greater risks of failure. There is no evidence, however, that this has occurred in the United States. U.S. government programs that speak to the Y2K issue are careful to note that the government cannot solve private sector problems. Liability issues also are central to the question of moral hazard and Y2K. If the producers and providers of information technology are believed by users to be legally liable for errors, user firms may do less to protect against failure.¹⁰ Some reports suggest that this may have been the initial position of some foreign governments. For instance, initial Chinese statements suggested that China would not make large efforts to fix Y2K errors and would shift the responsibility for failures to the foreign suppliers of Y2K deficient products. As Beijing and others have recognized the complexity of the issue–indeed China exports considerable volumes of information technology of its own—they have changed course and have encouraged their own firms and agencies to undertake Y2K fixes.



ASSESSMENTS OF Y2K READINESS IN THE UNITED STATES

Against this array of potential risks from Y2K, the United States by almost all assessments appears to be well prepared. While American firms and public agencies depend greatly on information technologies, and thus had great initial vulnerability, they began to address these risks earlier than firms and agencies in other countries. They also have spent tens of billions of dollars to identify and correct Y2K glitches.

Y2K Spending Estimates

Federal Reserve Board analysts and International Data Corporation (IDC) have developed useful, methodologically conservative estimates of total

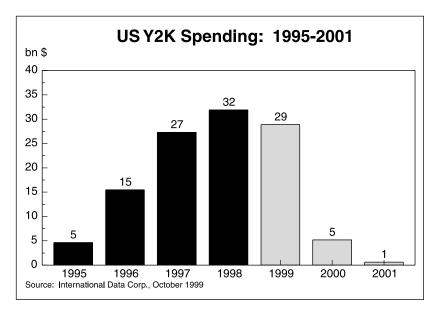
U.S. spending on Y2K. These estimates indicate that spending by U.S. firms, non-profits and government agencies, in the years 1995 through 2001, will be in the neighborhood of \$100 billion, or about \$365 per U.S. resident¹¹. According to the Federal reserve analysts, Y2K spending for the three years, 1998 - 2000, will total \$50 billion by the private sector, \$10 billion by the federal government, and \$5 billion by state and local governments. (To date, the federal government has budgeted \$8.3 billion for Y2K remediation.) The staff believes that their method for estimating business spending which is based upon 10-K and 10-Q filings with the Securities Exchange Commission represents a lower end figure and may understate total Y2K spending by the private sector.

International Data Corporation (IDC), in an October 1999 update for the U.S. Department of Commerce, estimates that over the seven year period 1995-2001, U.S. private and public spending

¹⁰ The aforementioned Y2K Act signed into law July 1, 1999 skirts this hazard by giving both suppliers of deficient technology and their customers reasons to share information and fix problems before they develop.

¹¹ These data cannot be highly precise since differentiating of Y2K spending from normal maintenance and upgrades of software and equipment, in many cases is difficult. The \$100 billion figure thus should be considered in terms of its significant digits. In other words we are confident that spending will total at least \$50 billion and that it is unlikely that it will be higher than \$150 billion.

on Y2K-software issues will come to \$114 billion.¹² This estimate reflects two first quarter 1999 surveys–one of 1,145 North American companies and the other of 1043 small businesses. These surveys cover private firms, non-profit organizations and government agencies, and cover all Y2K related IT spending, including internal and external services, hardware, and software. This estimate does not include non-IT Y2K-related expenses, such as legal fees or chips embedded in non-IT equipment.

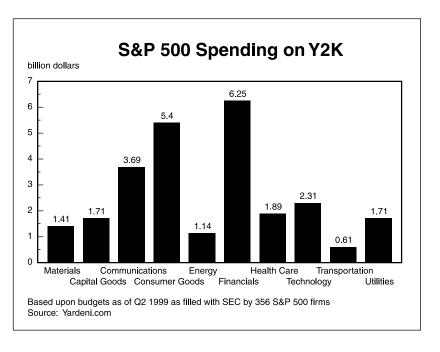


U.S. Y2K Spending, 1995-2001 (\$ Billions)

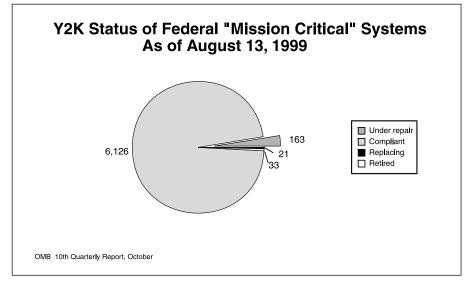
| 1995 | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | Total | |
|-------------------|------|------|------|------|------|------|-------|--|
| 4.6 | 15.5 | 27.3 | 31.9 | 28.9 | 5.2 | 0.6 | 114 | |
| Source: IDC, 1999 | | | | | | | | |

Other analysts have used data from filings with the Securities and Exchange Commission (SEC) to develop estimates by sector and industry. Edward Yardeni, an economist in Deutschbank, used SEC data for "S&P 500" companies, and established that highly IT-intensive industries with large potential effects on the rest of the economy are spending the most to correct Y2K problems. For instance, S&P 500 financialsector firms will spend \$6 billion on Y2K, the largest of any single sector. Industries and sectors with fewer direct linkages to other parts of the economy, such as education and health care, have spent relatively less.

These spending estimates provide a rough measure of Y2K costs already borne by the economy, but of course do not indicate whether serious Y2K risks to the economy remain.



¹² Azzara, Boggs, Oleson IDC Flash, "Updated Cost of Y2K in the United States: Special Report for the U.S. Department of Commerce," October 15, 1999. Funding courtesy of International Trade Administration, USDOC.



Economy-wide Assessments

A number of government and private organizations have recently published aggregate assessments of U.S. Y2K preparedness. For all the difficulties in making a national assessment, the Y2K problem is essentially a technological error that can be tested, observed, corrected and assessed. But important caveats remain. Much of the information used for these assessments comes from self-reporting by firms and agencies. There has been some use of independent verification procedures, usually required in financial and other critical

infrastructure sectors; but biases can affect overall results. Further, any organization can determine only its own readiness, and may not assess the impact of its own linkages to other organizations.

Federal Government Assessments

The Federal government has sponsored two major Y2K-assessment efforts, in addition to many agency and departmental based projects that are supervised by OMB. The Administration's official assessment of Y2K readiness is the responsibility of The President's Council on Y2K Conversion. The Council issues periodic assessments based upon evaluation of all available public and private information. In addition, the Senate Special Committee on the Year 2000 Technology Problem has issued its own assessments based upon hearings conducted over the last several years.¹³

The assessments released this year by the President's Council point to substantial progress in Y2K readiness in the United States, while noting the need for additional preparations in certain sectors. The "Second Summary of Assessment Information" issued in April, 1999 indicated that "substantial progress" had been made in the previous six-to-twelve months, finding that federal mission-critical systems would be ready and that national-level failures in key infrastructure, such as electric power, banking, telecommunications and transportation are "unlikely."¹⁴ The "Third Summary of Assessment Information" issued in August 1999 concluded that, "...additional evidence supports the Council's view that important national systems will make a successful transition to the Year 2000" and the Council had a "high degree of confidence" in the preparations by financial institutions, electric power, telecommunications, air travel and the federal government.¹⁵ In the "Fourth Summary" released November 10, the Council expressed continued confidence in U.S. populations. ¹⁶

Both of these reports also note that certain sectors are not fully prepared. The "Second Summary" stressed the "great risk" associated with organizations not paying appropriate attention to the problem or adopting a "wait and see" strategy, pointing to small businesses and local governments.

¹³ Investigating the Yar 2000 Problem: The 100 Day Report Senate Special Committee on the Year 2000 Technology Problem, page 1. ¹⁴ The President's Council on Year 2000 Conversion, *Second Summary of Assessment Information*, April, 1999, no pagination, from

[&]quot;Chairman's Summary."

¹⁵ The President's Council on Year 2000 Conversion, *Third Summary of Assessment Information*, August, 1999, no pagination, from "Overview."

¹⁶ The President's Council on Year 2000 Conversion, Fourth Summary of Assessment Information, November, 1999.

In the "Third Summary," the Council noted its continuing concerns about preparations by local government, health care and educational organizations, and small firms.

The Senate Committee's most recent report also notes the progress made, and, it too highlights areas of concern. The Committee's central point is that despite all the encouraging news, significant uncertainties remain. The Committee is particularly concerned about disruptions overseas affecting the U.S. economy.¹⁷

Private Sector Y2K Consultants

Private-sector consultants specializing in the Y2K issue have also been key sources of information for industry, government, and the public over the last several years. Of late, several of the major consultants have expressed optimistic views regarding U.S. Y2K readiness. The Gartner Group, which for several years raised alarms about the dangers of Y2K, reported in August that "We don't expect any real significant problems to the general public" on New Years and "(i)n fact, it's probably going to go by somewhat unnoticed" except for some isolated problems. The Gartner Group also indicated its view that small and medium-size companies have nearly caught up with larger firms in Y2K preparations.¹⁸

International Data Corporation (IDC) surveyed 1,145 firms in early-1999 and concluded that, "North America will meet the new millennium in good shape but not totally free from Y2K bugs." More than 85 percent of the firms surveyed were expected to complete their Y2K projects by the third quarter, and less than 10 percent of firms reported having no formal Y2K testing procedures. Among large companies only five percent reported having no formal procedures. IDC further concluded that two-thirds of the Y2K problems that do occur will "not cause significant business impact," and the remaining third "will be manageable."¹⁹ IDC estimates that only 0.2 percent of all Y2K bugs will cause business critical problems.²⁰

A third consultant, The Forrester Group, contacted major global firms and reports that those firms are 89 percent complete with initial repairs and 84 percent complete with final testing, and that only 5 percent of their applications will not be fully fixed and tested by January 1. The Forester Group also found that most global firms are also "putting contingency plans in place that include manual processes, infrastructure lockdowns, and material stockpiling"²¹ to protect themselves against disruptions. Finally, the Forrester evaluation confirmed that those industries that are most IT-dependent are also the industries with the highest levels of Y2K preparedness.

A July 1999 poll by the National Association of Manufacturers and Edward Yardeni (an outspoken skeptic of industry Y2K preparations) found that U.S. manufacturers are "confident about their ability to weather any Y2K storm." Some 97 percent of respondents believe that "the millennium bug will have zero or very minor impact on their companies," even though roughly one-third expect a small fraction of their critical systems to fail or malfunction. Most respondents (89 percent) were more optimistic than they had been just a month earlier, and 80 percent indicated

 ¹⁷ Investigating the Year 2000 Problem: The 100 Day Report Senate Special Committee on the Year 2000 Technology Problem, page 1.
¹⁸ Computerworld, "Gartner: Y2K Victory At Hand," Online News, August 17, 1999, quoting remarks by Lou Marcoccio in a teleconference on Gartner's final Y2K report of 1999..

¹⁹ Thomas D. Oleson and Carey V. Azzara, "Y2K: The End Is Near — IDC 1999 Survey Results," International Data Corporation, Executive Summary, quoted from pre-publication draft, expected publication date, September 1999.

²⁰ Frank Gens, "IDC Predictions '99: The 'Real' Internet Emerges," International Data Corporation, 1998.

²¹ Carl D. Howe, "The Y2K Hangover," Forrester Research, March, 1999.

that their own Y2K projects were already complete. The remainder were confident of completing their projects by the year's end.²²

U.S. VULNERABILITY TO Y2K PROBLEMS ABROAD

While confidence has grown about U.S. preparations for Y2K, many analysts remain concerned about the attention and resources devoted to the problem overseas. Some observers believe that foreign Y2K disruptions pose the greatest to the U.S. economy. For example, the Senate Committee's 100 Day Report, states:

While the Committee has become increasingly confident about U.S. Y2K preparedness, it has become increasingly concerned about international Y2K preparedness. Some of our leading trading partners are months behind in addressing the Y2K problem and are not likely to avoid significant disruptions. These disruptions could have adverse economic effects here at home, and, in some developing countries, result in request for humanitarian assistance.²³

Despite substantial globalization of the U.S. economy in recent years—exports account for about 11 percent of GDP and the value of our imports relative to GDP is 13 percent–US vulnerability to any particular region of the world is slight. The relatively small impact on the US economy of the very severe recession that hit East Asia in 1997 and 1998 is a good example.

Available evidence indicates that while foreign Y2K disruptions are expected, they likely will have only a transient effect on U.S. trade dependent sectors. However, foreign Y2K difficulties could adversely affect specific U.S. firms.

Virtually all international trade is conducted between private firms—often large multinational firms—that have incentives much like domestic American firms to correct Y2K problems.²⁴ For the most part, international trade involves longer supply lines, more inventory in train, and greater variety in supply sources and customers, than does most domestic exchange. The risks of disruption in finance, shipping, customs arrangements and other aspects vulnerable to Y2K problems is already part of the normal operations of firms engaged in foreign trade.²⁵ To firms engaged in foreign trade, it is not clear that Y2K is particularly different from other types of business risk. As in the domestic economy, however, the additional risk exists that many disruptions will occur at the same time, interfering with the ability of each firm to respond effectively. In addition, foreign critical infrastructure could fail, and present a cascading problem for a foreign economy. In such an event, demand for U.S. exports could weaken or our supplies of some import could be delayed. Depending on the circumstances, a disruption in the supply of some import could actually boost demand for alternative U.S. suppliers.

²² National Association of Manufacturers, Press Release 99-239, "New NAM-Yardeni Poll Shows Major Manufacturers Optimistic About Overcoming Millennium Bug," July 15, 1999.

²³ Senate Committee, Executive Summary, page 2.

²⁴ Mary Cripe, project manager 3-M; "Our overseas companies are doing a very thorough job. My concern is that the surrounding governments and business partners they deal with have not recognized remediation as a high priority as in the US. Of particular concern is the number of foreign infrastructure that are operated by government agencies rather than private corporations. PC Labs, July 12. PC Week Online

²⁵ "World's 20 busiest seaports may experience y2k delays averaging 12 days. International Monitoring Ltd. London. PC Labs, July 12. *PC Week Online*.

Assessments of Foreign Preparedness

Several U.S. and international organizations have attempted to review the state of Y2K preparations in countries around the world for a variety of reasons, including guidance to travelers regarding the safety of foreign public infrastructure.²⁶ Generally these reviews have not been intended to predict the economic repercussions from Y2K problems in these countries, much less to forecast the implications of any such repercussions for the U.S. economy.²⁷ However, these reviews can provide useful information focusing on the level of knowledge about Y2K matters in given countries and on mechanisms being used to fix the problem.

In addition, the National Intelligence Council (NIC) provided a useful summary of the US Intelligence Community's assessment of the impact of foreign Y2K problems in Congressional testimony of October 13th. The NIC concludes that whereas all countries will experience Y2K related problems, they are not likely to have a major impact on the U.S. or the world economy.²⁸ The Intelligence Community predicts that communications disruptions abroad could affect some U.S. firms, but not to a serious degree and that global payments system are unlikely to experience significant failures. The United States is unlikely to experience a significant problem with oil deliveries (although prices could rise temporarily as disruptions occur elsewhere). The NIC also concluded that natural gas disruptions overseas should not affect the United States in any significant way, and that while some European countries may experience localized electricity blackouts, cascading failures were highly unlikely. Further, the shipping industry is unlikely to experience significant Y2K-related disruptions. However, the NIC believes that countries with extensive inventories of Soviet equipment may be particularly vulnerable; and that Russia is in a unique class in terms of the potential scope and persistence of Y2K failures.

Assessing the threat to the U.S. macro economy from Y2K problem abroad involves four issues. First, to what degree is a foreign economy dependent on Y2K-vulnerable technology? Second, how prepared is the foreign country for Y2K? Third, what is the importance of specific industries in a foreign economy to specific American industries? Fourth, what is the nature and extent of Y2K problems for specific industries abroad that are linked closely to specific industries in the United States? For foreign Y2K failures to present a threat to the U.S. economy, all four factors must be present and substantial — the U.S. economy could be put at risk only by a vulnerable and poorly-prepared economy that is very important to the U.S. economy and which carries large Y2K-related links to the US.

An examination of important U.S. trading partners from this perspective, using assessments provided by State Department, the World Bank, the Group 2000 of the Bank of International Settlements in addition to the NIC finds *no country* where all four risk factors are present and working against the U.S. Generally, wherever information technology plays a significant role in an economy, Y2K preparations are reasonably strong.

²⁶ The US Department of State, for instance, has engaged in a intensive assessment of foreign country risks and reactions to the Y2K problem. See www.statey2k.com.

²⁷ Given the very high level of aggregation that is involved in these assessments, the Gartner Group cautions clients that, for business decisions, "specific data about specific companies or sectors must be used, not high-level data." Aggregate country-level readiness assessments provide a starting point for investigation or contingency planning and should not substitute for the "tedious–but absolutely necessary–task of having each of their business groups…undertake its own risk analysis." Similarly, for purposes of analyzing the

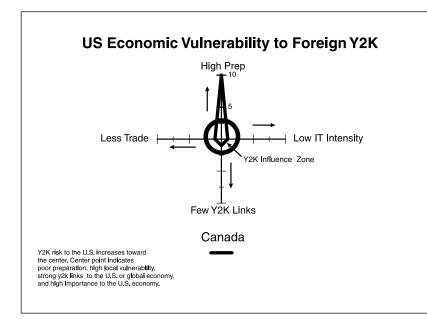
economic implications of overseas readiness, these aggregate country level assessments should be treated as providing only an indication of risk, not as a specific probability estimate that can be confidently used for a quantitative assessment.

²⁸ Congressional Testimony, October 13, 1999.

Even if disruptions in trade with some countries did occur, the impact on the overall U.S. economy would be slight. Not only do both exports and imports each represent comparatively small shares of the entire economy, but also both exports and imports are highly diversified across more than 200 trading partners and tens of thousands of foreign firms. And approximately 27 percent of U.S. foreign trade is conducted with overseas affiliates of U.S. firms whose parents presumably have a high stake in fixing their overseas Y2K issues. The countries and firms with which U.S. firms trade the most–Canada, Japan, Mexico and Europe—are generally reported to be well prepared.²⁹

For illustrative purposes, assessments of four countries that pose different classes of Y2K risks to the U.S. economy are presented below using a 4 quadrant graphic to relate these risks to each other. In these graphics, a country that posed a large Y2K risk to the US economy would show as a small area entirely enclosed by the circle. A country that posed less of a threat would have one or more points far outside of that circle.

The **Canadian** economy is IT-intensive and therefore inherently vulnerable to IT failures. It is also very important to the United States, both in terms of the extent of our trade relations and in terms of extensive Y2K-related linkages. These three risk factors are shown as points close to the center



of the graphic. But, by all reports, Canada has worked very hard to prepare for Y2K, as could be expected given its latent vulnerability. The high level of preparation thus greatly lowers that country's risk to the US economy.

But assessments that focus only on a country's state of preparation cannot provide a full picture of potential U.S. vulnerabilities. Extensive preparation does not mean that a country will not experience disruptions. If such disruptions occur in sectors with close links to the United States, U.S. firms could be affected.

The graphs of other G-7 countries, as well as Mexico, are similar, and probably do not pose any greater danger than Canada. Most would be considered slightly less well-prepared than Canada, but also less important to the U.S. as a

trading partner and with fewer direct Y2K links to the United States. Japan and Germany were seen as late starters in their Y2K fixes but international reports suggest that they have been catching up. It is also worth noting that from each of these countries perspectives–especially Canada's—the U.S. may represent one of their largest foreign Y2K risks.

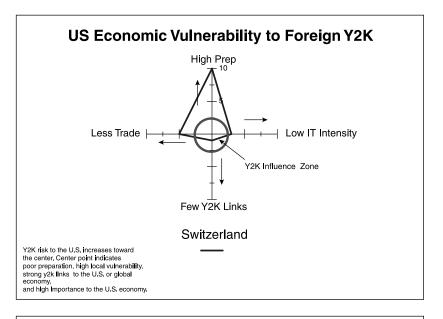
Switzerland presents a different type of potential risk to the U.S. economy, one with extensive links. Like Canada, the Swiss economy is highly IT-intensive, as noted in the center point on the right hand (x) axis, and has extensive Y2K related links to the United States, especially in finance, as noted in the close to the center lower (y) axis. For instance, significant Y2K problems in Swiss banking could increase worldwide demand for liquidity and reduce demand for Swiss francs,

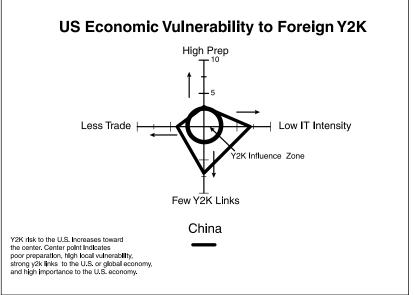
²⁹ See U.S. Department of Commerce, International Trade Administration "The Year 2000 Problem and the Global Trading System" for further analysis of trade vulnerabilities.

which in turn could affect the U.S. economy by putting upward pressure on the dollar. Despite these dangers, the Swiss economy is reported to be very well prepared for Y2K and ultimately is quite small and not very important to the U.S. economy. Barely 1 percent of U.S. exports go to Switzerland, and only 1 percent of our imports come from Switzerland.

Other financial and trade centers such as Hong Kong, Singapore, and perhaps Belgium/ Netherlands, pose similar issues. Each have been very highly rated in terms of Y2K preparedness.

China presents a different kind of Y2K risk to the United States. State Department and other reporting suggest that China is not as prepared for Y2K problems as are our other major trading partners, including problems in some critical infrastructure such as power plants. However, China's economy is generally not very ITintensive, and coastal areas, where IT usage is more intensive, are reported to be better prepared. Significant risks to the Chinese economy probably include equipment and facilities provided by defunct Soviet and East European firms, and poorly-managed software used by large state owned enterprises. However, there are few channels through which any such disruptions could be transmitted to the U.S. economy. U.S. imports from China, \$71 billion in 1998, are largely consumer goods or producer goods for which other sources could provide reasonable substitutes albeit at higher prices. U.S. exports to China, \$14.2 billion in 1998, represent only 2.1

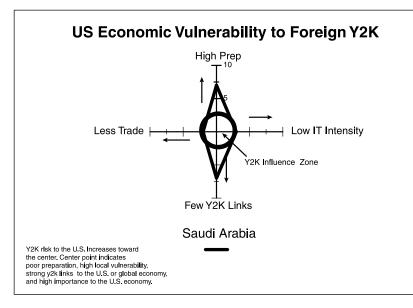




percent of our total exports, and only 0.2 percent of our GDP.³⁰

Russia and several eastern European countries are probably even less prepared but carry less economic risks for the United States. U.S. exports to Russia, for instance, through August of 1999, amounted to less than 0.2 percent of US exports and an insignificant share of GDP.

³⁰ One such link eventually may include litigation: China initially claimed that Y2K errors in equipment imported from abroad are the responsibility of the seller to identify and correct–an attitude that may seem to be defensible but also delayed firms and agencies from taking control of their own vulnerabilities.



Saudi Arabia, the world's largest supplier of crude oil, poses yet another type of risk. If Y2K problems in production, distribution, or finance significantly reduce supply on world oil markets, oil prices could become volatile, spilling over into other energy areas. For this reason we attach a very high degree of economic importance to Saudi Arabia. But the oil industry itself is said to be very well prepared for Y2K, and other related linkages are quite modest.³¹

Cross-Cutting International Industry Issues

In addition to specific foreign country issues, questions have been raised about the potential impact on the United States of Y2K problems in transportation maritime shipping and ports

particular global industries: petroleum, air transportation, maritime shipping and ports, telecommunications, and international finance.

Petroleum. One common trade-related concern has been potential U.S. economic vulnerability to disruptions in oil supplies, as occurred during the 1973 OPEC oil embargo and its aftermath. It is worth noting that the United States imports today a larger share of its total petroleum consumption than in the 1970s. One of the few analysts who has forecast a worldwide recession as a result of Y2K problems, Edward Yardeni of Deutschbank America, gives as primary reason a disruption in world oil supply.³²

The oil industry and others strongly challenge this view. First, even if Y2K problems interrupted shipments of oil supplies, there is no reason to believe such disruptions would last more than a few days or weeks. With large stocks of oil in transit and in storage at any given time, and very flexible prices, there should be little long-term impact on the U.S. The American Petroleum Institute, in a report released in August, concurs in very strong terms:

Y2K assessments that predict shortages of petroleum products have no basis in fact. Almost all American petroleum firms - and key foreign suppliers like the national oil company of Venezuela - are on or ahead of schedule to be Y2K compliant. Comparisons of Y2K problems to the panic conditions and chaos of the 1970s result from misperception ...³³

Air Transportation. Air transportation to and from the United States may experience isolated service disruptions that could subject passengers to inconvenient delays or diversions while traveling either domestically or abroad, according to the FAA. To date, the FAA has not identified any aircraft safety problems associated with Y2K which would justify prohibition of aircraft from U.S. airspace. And, according to the Air Transportation Association, as of September 30, 1999, major U.S. airlines had completed 99 percent of their overall remediation and testing work and 85 percent of contingency planning. The 20 major U.S. airports which handle nearly all

³¹ "Tackling the Year 2000 Problem", American Petroleum Institute, 9/3/1999.

³² See www.yardeni.com

³³ "Tackling the Year 2000 Problem", American Petroleum Institute, 9/3/1999.

international travel to and from this country will complete their Y2K repair process by the end of November.³⁴

Internationally, links with the United States also appear to be in relatively good shape. Eighty two percent of the member states of the International Civil Air Organization, representing 99 percent of total international air traffic, had reported by October 30 that their air transportation systems are or will be ready by the century date changeover. The ICAO notes that each of the 50 largest carriers and each of the 25 largest international airports have filed responses indicating they are making progress against the century date change. ³⁵ Further analysis of data submitted by these organizations will be made available by the ICAO.

The FAA points out that the whole Y2K phenomenon is characterized by uncertainty as to its affects and that all U.S. air carriers must continue to adhere to the Federal Aviation Regulations. In the event adverse conditions are expected, contingency plans will be required which might include additional fuel, use of alternate airports, restrictions on operations to daylight only etc. Nonetheless, air carriers encounter many types of adverse conditions around the world every day and the century date changeover is anticipated to be little different.³⁶

Maritime Shipping and Ports. The United States Coast Guard has the leadership role for ensuring that U.S. ports and shipping are prepared for Y2K, and that the U.S. helps the international maritime community prepare. In recent testimony before the Senate Special Committee, U.S.C.G. Rear Admiral George Naccara reported that government-contracted surveys show "a high level of Y2K preparation in the shipping industry, and a steadily improving picture in the world's ports." However, some risk and uncertainty remains, reflecting the industry's dependence on information technologies, particularly embedded chips. Further, analysts express higher levels of concern about some foreign ports.³⁷

Telecommunications. Most assessments of Y2K readiness in international telecommunications Y2K are optimistic. The International Telecommunications Union (ITU) has concluded that it is, "unlikely that there will be material disruption to the telecommunications network in terms of call connectivity" because there is "very little date information passed across the interfaces in real time." Telecommunications equipment does make significant use of embedded chips, however. One matter of concern is the "possibility of congestion at the time of the century date change with an increased level of calls and customers checking for dial tone." The ITU task force "remains of the view that major players and their major trading partners are not likely to see significant disruption to service as a direct result of Y2K." ³⁸

Similarly, the FCC's Network Reliability and Interoperability Council (NRIC) released a report on July 21, 1999 updating its risk profile for international telecommunications networks. The NRIC noted substantial progress in the industry's Y2K readiness. Overall, the NRIC reported that its testing "indicated the risk of international call failure between the North American region and

³⁴ President's Council on Year 2000 Conversion, *Fourth Summary of Assessment Information*, November 10, 1999; page 72. ³⁵ See ICAO web page at http://icao.int/y2k

³⁶ As a public service, the DOT/FAA is maintaining information on domestic and international destinations frequently visited by U.S. citizens which can be reached at the DOT web site, www.fly2k.dot.gov

³⁷ Rear Admiral George Naccara, testimony on "Maritime Y2K Readiness," before the Senate Special Committee on the Year 2000 Technology Problem, September 30, 1999, http://www.cnoy2k.navy.mil/ny2k/ny2k.htm

³⁸ International Telecommunications Union (ITU) Study Group 2, Year 2000 Task Force, Statement to the U.S. Senate Special Committee on the Year 2000 Technology Problem," July 22, 1999, www.senate.gov/~y2k/hearings/990722/itu.htm .

other World regions is minimal," although network congestion may occur at the century date change.³⁹

International Finance. International financial institutions were among the first to begin Y2K programs, and most analysts and reports have concluded that there is little likelihood of financial-sector disruptions that could significantly affect transactions with the United States. A highly successful series of cross-border payment systems tests conducted across 34 national and international payments systems and 500 financial institutions, coordinated by the Global 2000 Committee of the Bank of International Settlements is strong evidence that such systems are not likely to be a source of instability during the century date change.

The Global 2000 Committee, chaired by Federal Reserve Vice Chairman Roger Ferguson, is highly optimistic regarding U.S. and other developed country preparedness but like most international organizations, lacks data and reporting on the situation is many less developed regions of the world. In a highly optimistic statement of preparations made by U.S. financial institutions in October, 1999, Vice Chairman Ferguson reported:

"No one can declare with certainty how the millennium rollover will unfold internationally, and much of my information is anecdotal. However, the financial service sector is generally perceived to be better prepared than other sectors in almost every country. In general, I can report that the financial firms of the developed countries, like those in the United States, either are, or appear to be making good progress toward being prepared. Similarly, the financial institutions of a number of transitional economies are well advanced. The financial institutions that are thought to have the furthest to go, in general, are those in countries that are least dependent on technology. They have the greatest experience with frequent disruptions of the type that one might expect during the changeover period and can most easily return to manual workarounds or other contingency plans."⁴⁰

³⁹ Network Reliability and Interoperability Council (NIRC), "U.S. Telecommunications Industry Nears Year 2000 Readiness," www.nric.org/press-release/1999july21.html, July 21, 1999.

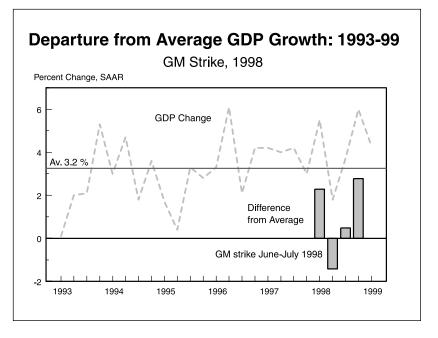
⁴⁰ October 6, 1999 :"Year 2000: Eighty-six Days and Counting". Speech to National Association of Federal Credit Unions.

CONCLUSION: DIRECT EFFECTS OF Y2K ON THE AMERICAN ECONOMY

The American economy, as well prepared and resilient as it is, still is likely to feel some impact from the century date change. No one can predict with certainty the dimensions of these effects; in some cases predicting even the direction of change is difficult. However, certain aspects of economic activity could exhibit Y2K effects — in particular, effects on output, inventories and investment, and consumer responses.

Disrupted Output

Y2K problems could clearly disrupt production of some goods and services, but there is no consensus over how much production is likely to be lost. Much of the discussion focuses on the potential for dramatic disruptions in "critical" industries. All available evidence indicates that such disruptions will be very rare in the United



States, if they occur at all. There is greater likelihood of minor disruptions in production in a number of places, affecting the productivity and profitability of some firms for a short period, and possibly the prices of some products. The effects of such disruptions likely would show up in the monthly measures of industrial production and retail sales for January or February of 2000, or possibly export and import data.

Production disruptions are likely to have only transient affects on U.S. economic growth. Most industries will be closed for the New Year's holiday period, providing several days to work out problems. Moreover, despite a robust economy, most U.S. industries are not operating near their peak capacities, much less near their surge capacity. If such minor disruptions do occur, most firms will be able to compensate by increasing production in succeeding weeks and months. Electric power demand, for example, draws only 40 percent of its capacity in January, although regional variations exist.

The 1998 work stoppage in General Motors assembly plants is an example of a major output disruption. At the peak, 110,000 auto workers were out of work. Industrial production plummeted in July and August, and GDP slowed to 1.8 percent growth from 5.5 percent the previous quarter. Once the work stoppage ended, production resumed at a higher pace and GDP output for the year was virtually unaffected — 3.9 percent growth, exactly the same rate as in 1997.

Another relevant example of an output disruption caused is the recent earthquake that hit central Taiwan causing massive disruption in that country's important semiconductor and computer component industry. Prices of semiconductor chips jumped initially as world demand is near world capacity and downstream assembly of computers may be affected as the supply of key components remains strained. Such an event clearly has short term repercussions for individual

U.S. computer companies and consumers but ultimately is quite short-lived with little or no overall U.S. impact on the U.S. economy.

For output disruptions to create an economy-wide or long-term problem, the problems are most likely to occur in an industry that is extensively linked to other parts of the economy and dominated by a few large firms. With few exceptions, in the United States even so-called "critical" industries include a great deal of competing systems created by deregulation and technological advancements in recent decades.

• One exception is distribution of electric power. However, there are some 3,000 local electric powers utilities in the United States, linked together to form three major power grids that provide substantial redundancy. While the likelihood of individual breakdowns is probably higher during the century-date change than normal times, the prospects of a cascading problem are highly remote.

As a general rule, the linkages that can make an economy vulnerable to Y2K effects are accompanied by high levels of competition that make modern systems highly redundant and resilient, compared to the serial or closed systems of the past. For example, modern payments systems–credit cards, money cards, debit cards, checks and cash–include many alternatives for commercial transactions. Modern telecommunications and transportation systems also incorporate considerable redundancy. Moreover, the competitive forces that create such redundancies also create incentives for firms, especially highly-linked ones, to fix any potential Y2K problems.

Y2K Inventory Shifts.

Most analysts expect some Y2K-related inventory stockpiling to occur in the second half of 1999, as firms put in place Y2K contingency plans to cope with possible shortfalls of inputs, and as some consumers stockpile emergency goods. After the New Year, these inventories will be drawn down. Since GDP measures the flow of production, not of final consumption, this analysis suggests that additions to inventory will add slightly to GDP growth in the fourth quarter of 1999, and subtract from GDP in the first quarter of 2000 as both the rate of inventory growth slows and turns negative for stocks being drawn down. This cycle could add to GDP growth again in second quarter of 2000, as the draw-down ends.

If these effects occur, they would change the timing of GDP growth but not its final levels. A recent survey of purchasing managers indicated that significant numbers have plans to add inventory in late-1999 beyond that normally added prior to the holidays. However, so far no evidence of Y2K inventory buildup has appeared in the statistics. In fact, inventories per unit of sales fell through July and August to cyclical lows. Therefore, a pick up in inventory accumulation this winter might be expected, even without Y2K.

American businesses probably have more reason for concern about potential Y2K supply problems from foreign producers than from domestic ones. As a result, inventories of imported goods could increase more than the inventories of domestic goods. This would reduce the Y2K-related variations in GDP, but create a similar swing in the flow of imports.

Consumer Responses

It is difficult to say with any confidence how consumer behavior may shift in response to Y2K concerns. Much like businesses, in late-1999 some households will likely accumulate stocks of items whose supply they do not want interrupted, and subsequently reduce their purchases of those items in early 2000. On the other hand, Y2K-inspired caution may lead some people to spend less as the New Year approaches. Current polls suggest that the public is becoming less worried about Y2K as the date approaches.

Y2K pundits advice on how to handle Y2K typically includes recommendations that people withdraw a little more cash at the end of the year than they would for a normal New Year's weekend, despite the fact that financial institutions have invested more intensively in fixing Y2K problems than any other industry. Without abetting such behavior, the nation's monetary authorities and private financial institutions have made extensive preparations to ensure sufficient liquidity, should the demand for cash increase. Obviously, a widespread movement by the American public towards more liquidity and cash could have important impacts on financial markets but whether this would add or subtract from overall economic activity–as measured by GDP—is not clear. For example, a substantial shift from financial assets to cash could lower the prices of those assets, increasing their returns, while an increase in debt to hold cash could raise interest rates. Similarly, there would be no effect on overall spending if the cash came from bank accounts and was then returned. But if the additional cash came from saving accounts, and some portion of it were spent, it could, in fact, boost GDP in the first quarter of 2000.

The Costs of Fixing Y2K.

The most significant economic impact of Y2K on the U.S. economy is most likely to be the costs incurred to protect ourselves against the problems, and most of that cost has already been paid. As noted earlier, estimates of these costs have run about \$30 billion a year in 1998 and 1999 and a cumulative cost in the neighborhood of \$100 billion for the period 1995 through 2001. Fixing Y2K glitches has spared the economy many potential disruptions, but at a cost of diverting resources from other purposes. As the Y2K repair burden ends, thousands of workers skilled in programming and systems analysis, and billions of investment dollars, will be able to shift to uses that raise the productivity and future living standards of Americans.

As information technology spending shifts from the intensive fixing of Y2K issues to a likely waiting or "lock-out" period in these last months of 1999 as firms don't want to disturb tested systems, to accelerated spending next year on new technologies that have been held up by Y2K programs, quarterly shifts in GDP investment data may occur. Some firms will see important shifts in demand for their products in the fourth and first quarters, as IBM indicated in its third quarter profits report. Deployment of IBM's more complex systems have definitely slowed in the third quarter and may remain down in the fourth quarter as firms don't want to complicate their Y2K fixes until after the New Year.⁴¹

Summing up, The Impact on GDP

Despite all the unavoidable uncertainties, many economists have no choice but to try to estimate the impact of Y2K on the overall U.S. economy as they prepare their normal short-term forecasts.

⁴¹ "IBM Y2K Woes May Hurt Market', By Bruce Meyerson AP Business Writer, October 21, 1999

A few analysts have explicitly isolated the Y2K impact; most forecasters weave Y2K effects into the many other issues confronting the economy. On average, these forecasters expect a slight Y2K-related boost to GDP in the second half of 1999, followed by a comparable Y2K-related subtraction from GDP in the first quarter of 2000. For most, the net result over the course of a year is virtually nil.

A May 1999 survey of 37 forecasters by the Federal Reserve Bank of Philadelphia is representative. These forecasters anticipate an average 1999 gain from Y2K of 0.3 percent followed by a 0.3 percent subtraction in 2000. The largest factors in this effect would be inventory accumulation and changes in the timing of capital purchases (including personal computers). The second most important potential cause of problems found in the survey was foreign problems that could lead to disruptions in U.S. production. Economic costs due to the failure of domestic systems or to consumer stockpiling did not figure prominently in the forecasters' views.⁴²

The Wall Street Journal conducted a similar survey of 54 economists in the second quarter of 1999, and found that the members of that group, on average, believed that Y2K would add about 0.4 percentage point to growth in the second half of 1999 and cut GDP growth by nearly 0.7 percent in the first half of next year. These economists, however, divided sharply into those who foresee no aggregate impact at all and those that believe there will be measurable effects. Those in the second camp expect higher business spending in the second half of 1999, on capital goods and inventory, and lower spending in 2000, with computer purchases completed and inventories overstocked.⁴³

Consensus-type estimates rarely capture turning points in an economy and the art of economic forecasting is particularly weak in estimating the impact of one-time events, nevertheless these forecasts are encouraging.

Whatever the magnitude of the Y2K effect on the aggregate U.S. economy over the next few quarters, it is highly unlikely that Y2K problems would last long enough to affect the level of GDP that is likely to be achieved by the end of 2000. If there is any certainty in Y2K, it is that by early 2000 a much more clear view of the impact will be available.

⁴⁴ Federal Reserve Bank of Philadelphia, "Survey of Professional Forecasters," May 21, 1999.

⁴³ Constance Miller Ford, "Economists Expect Strong Growth for 1999 But Are Mixed on 2000," Wall Street Journal Highlights, July 2, 1999.

